UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/281,852	03/31/1999	DARYL CARVIS CROMER	RP9-99-048	7708

7590 05/21/2004

BRACEWELL & PATTERSON, L.L.P.
INTELLECTUAL PROPERTY LAW
P.O. BOX 969
AUSTIN,, TX 78767-0969

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 05/21/2004

17

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/281,852	CROMER ET AL.	
	Examiner	Art Unit	
	Thanhnga Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 10-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 10-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-7 and 10-16 are rejected under 35 U.S.C. 102(e) as being unpatentable over Win et al (US 6, 161, 139), and further in view of Shrader et al (US 6, 374, 359 B1).

a. *Referring to claim 1:*

i. Win teaches:

(1) in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key **[i.e., if the name and password are correct, the Authentication Client Module reads the user's roles from the Registry Server 108. It then encrypts and sends this information in a "cookie" to the user's browser. A "cookie" is a packet of data sent by web servers to web browsers (column 6, lines 51-56). In addition, As shown by state 524, cookie 528 and cookie 530 are encrypted and returned to the browser 100. Alternatively, state 524 may involve digitally signing cookie 528 and cookie 530 using a digital signature algorithm. Preferably, the cookies are encrypted rather than digitally signed because encryption is faster and produces a smaller cookie (column 11, lines 1-8)];**

(2) storing said encrypted cookie in a non-protected storage device within said data processing system **[i.e., referring to Figure 5C, cookie 528 and cookie 530 are saved in memory by the browser 100 indefinitely, unless either of the cookies expires, i.e., the system clock becomes equal to or greater than the expiration date value. The cookies 528, 530 are passed to each Web**

server that the user accesses and that is within the same domain as the Access Server 106. When a user quits the browser 100, cookies that have not expired are saved on a mass storage device associated with the browser 100, such as a disk drive located at the user's client machine or terminal (column 11, lines 11-18)];

(3) in response to an access request for said encrypted cookie by a browser program executing within said data processing system, decrypting said encrypted cookie with said private key **[i.e., when the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource (column 6, lines 65-67 through column 7, lines 1-3)]**; and

(4) sending said decrypted cookie to said browser program **[i.e., the cookie is also used by the resource to return information that is customized based on the user's name and roles (column 7, lines 3-5)].**

ii. Although Win does not explicitly explain:

(1) storing a encryption key pair having a private key and a public key in a protected storage device within said data processing system **[i.e., all transactions between components in the system are made using HTTP over SSL (Secure Sockets Layer) sessions. For example, browser 100 initiates an SSL session with a handshake during which it negotiates a hash function and session encryption key, that is "having a private key and a public key" with HTTP Server 402 of Access Server 106, that is "a protected storage device" for "storing a encryption key pair having a private key and a public key". Once the session is established, all data exchanged between browser 100 and HTTP server 402 is encrypted (column 22, lines 66-67 through column 23, lines 1-5)]**;

iii. Shrader, on the other hand, teaches:

(1) The key may comprise part of a public key cryptosystem (PKC - that is to employ an encryption key pair, such as a decryption private key and an encryption public key to decrypt and encrypt data), with the

corresponding key being used for decryption in a known manner. A representative software PKC product is known in the art as PGP (Pretty Good Privacy), which is available for download over the Internet. Other encryption techniques, such as a private key cryptosystem using a session key, or the like, may be used as well. Preferably, the key pair is constructed and stored locally (for root user access only) during configuration of the Web server **(column 7, lines 23-32)**.

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly disclose the storing of an encryption key pair for authenticating users of the access system 2 as in Figure 1 of Win.

v. The ordinary skilled person would have been motivated to:

(1) clearly disclose the storing of an encryption key pair for controlling access to protected information resources in a network environment, more specifically to methods, apparatus, and products for facilitating secure and selective access to network resources based on a role of a user of the resources **(column 1, lines 5-10 of Win).**

b. *Referring to claim 2:*

i. Win further teaches:

(1) wherein said non-protected storage device is a hard drive **[i.e., referring to Figure 9, a storage device 910, such as a magnetic disk, that is "a non-protected storage device", or optical disk (column 26, lines 17-18). In fact, a mass storage device associated with the browser 100, such as a disk drive, that is also "a non-protected storage device", located at the user's client machine or terminal (column 11, lines 16-18)]**.

b. *Referring to claim 3:*

i. Win further teaches:

(1) further comprising providing an encryption device having an encryption engine and said protected storage device accessible only through said encryption engine **[i.e., all transactions between components in the system are made using HTTP over SSL (Secure Sockets Layer) sessions. For example,**

browser 100 initiates an SSL session with a handshake during which it negotiates a hash function and session encryption key with HTTP Server 402 of Access Server 106. Once the session is established, all data exchanged between browser 100 and HTTP server 402 is encrypted. The SSL hash function is used to ensure data integrity, that is, to ensure that transactions are not tampered with or altered in any way. SSL encryption (that is "an encryption device having an encryption engine") is used to ensure that each transaction is private and confidential. This means that no one can wiretap or eavesdrop and read the contents of transactions. Thus no one can intercept names, passwords and cookies (column 22, lines 66-67 through column 23, lines 1-12)].

c. *Referring to claims 4, 5, 6, 7, 13, 14, 15, and 16:*

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

d. *Referring to claim 10:*

i. This claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

e. *Referring to claim 12:*

i. This claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

Response to Argument

3. Applicant's arguments filed March 22, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"Since Win teaches the encryption of a cookie is performed within a server instead of a data processing system remotely located from the server, the claimed encrypting step is distinguished from the teachings of Win."

Examiner maintains that:

In addition to the rejection, Win also teaches in one embodiment, all the components are stored on and executed by one physical server or computer. In alternate embodiments, one ore more components are installed on separate computers;

this approach may improve security and performance. For example, Registry Server 108 may be part of a secure Intranet that is protected using a firewall 118, and Access Server 106 may be located on an extranet (that is remotely located) for access by users inside and outside the enterprise. Further, there may be more than one Registry Server 108 in a mirrored or replicated configuration. Each Access Server 106 may be coupled to more than one Registry Server 108, so that a particular Access Server 106 can communicate with a second Registry Server 108 if a first one is busy or unavailable. Each Registry Server 108 may be coupled to or support more than one Access Server 106 (column 4, lines 56-67 through column 5, lines 1-3). Besides, in reviewing the claimed language, "in response to the receipt of a cookie generated by an application from a remote server, encrypting said cookie with said public key", as set forth in claim 1, this claimed language does not recite that the encryption system is performed at a server or at a data processing system since both server and data processing system can respond to the receipt of a cookie.

Applicant further argues that:

"Hence, even if the storing of cookies in a memory was disclosed by Win, Win was referring to the storing of cookies in a server and not in a data processing system, as claimed. Shrader does not teach or suggest the claimed storing step either."

Examiner maintains that:

Data processing system, by definition, is just a computer system which processes information after it has been encoded into data (see Wikipedia, the free encyclopedia). Furthermore, an assembly of computer hardware, firmware and software configured for the purpose of performing various operations on digital information elements with a minimum of human intervention (see Terminology Reference System). A server, by definition, (1) on a local area network (LAN) is also just another computer system for running administrative software that control access to the network and its resources, such as printer and disk drives, and provides resources to computers functioning as workstation on the network, (2) on the internet or other network, a computer or program that respond to command from a client. For example, a file server may contain an archive of data or program file; when a client submits a

request for a file, the server transfers a copy of the file to client (see Microsoft Computer Dictionary, Fifth Edition). Therefore, data processing system and server have the same function and meaning. Win and Shrader, in combination, teach encryption key pair, which is public key and private key, whereby the Access Server of Win is for storing the encryption key. Examiner maintains that a sufficient reason of combining has been given in the rejection, and recited in this rejection to claims 1 and 10 again.

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
May 17, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100